



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|--|-------------|----------------------|---------------------|------------------|
| 09/810,288 | 03/16/2001 | Wei Dong Kou | CA920000054US1 | 5926 |
| 38424 | 7590 | 12/14/2005 | EXAMINER | |
| DUKE W. YEE YEE & ASSOCIATES, P.C. P.O. BOX 802333 DALLAS, TX 75380 | | | SON, LINH L D | |
| | | | ART UNIT | PAPER NUMBER |
| | | | 2135 | |

DATE MAILED: 12/14/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

| | | | |
|------------------------------|--------------------------------------|-----------------------------------|--|
| Office Action Summary | Application No. 09/810,288 | Applicant(s) KOU ET AL. | |
| | Examiner Linh LD Son | Art Unit 2135 | |

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 23 August 2005.
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-31 and 33 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-31 and 33 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date <u>06/06/05</u> . | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. This Office Action is responding to the Appeal Brief received on 08/23/05.
2. An appeal conference has met and fully considered applicants' remarks in the Appeal Brief. The Conferees agreed with the applicants on the remark on the page 22 regarding to the limitation of "utilizations of the authcode cookie that are interspersed between utilizations of the session cookie". However, a newly found prior art has brought the pending claims 1-31, and 33 to the rejection below. Examiner provides a new ground of rejection below for claims 1-31, and 33.
3. Reopening of Prosecution - New Ground of Rejection After Appeal or Examiner's Rebuttal of Reply Brief In view of the Appeal Brief filed on 08/23/05, PROSECUTION IS HEREBY REOPENED. A new ground of rejection is set forth below. To avoid abandonment of the application, appellant must exercise one of the following two options: (1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or, (2) request reinstatement of the appeal. If reinstatement of the appeal is requested, such request must be accompanied by a supplemental appeal brief, but no new amendments, affidavits (37 CFR 1.130, 1.131 or 1.132) or other evidence are permitted. See 37 CFR 1.193(b)(2).
4. Claims 1-31, and 33 are pending. Claims 32 and 34 are canceled.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. Claims 1-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wood et al, US/6892307B1, hereinafter "Wood".

7. As per claims 1:

Wood discloses "A method of secure session management and authentication between a web site and a web client, said web site having secure and non-secure web pages, said method comprising the steps of: utilizing a non-secure communication protocol and a session cookie when said web client requests access to said non-secure web pages" in (Fig. 1, Col 5 lines 1-40, Col 8 lines 23-67);

The session cookie in Wood is the session cookie that has a low credential or trust level (Col 9 lines 20-25), and the authcode cookie is also the session cookie that has a high credential or trust level and the authentication information is encrypted (Col 8 line 65 to Col 9 line 25). Wood discloses in Col 8 lines 3-18 that the environmental information of the session (i.e. browser type, encryption capability, connection type and more) is used in some configurations for mapping particular authentication mechanisms to trust levels and for authorization decisions.

As evidence above, Wood teaches “utilizing a secure communication protocol and creating an authcode cookie when said web client requests access to said secure web pages”. The secure communication protocol is the encrypted communication session environment in Col 8 lines 3-18.

Wood also further discloses “so that utilizations of said authcode cookie are interspersed between utilizations of said session cookie, and at least some utilizations of said session cookie take place after utilizations of said authcode cookie” in (Col 10 line 58 to Col 11 line 13, Col 13 lines 1-19, and Col 15 lines 1-57). Implementing multiple cookies or tokens allow access different credential level or trust level resources (Col 8 lines 15-55) with respect to the environmental information of the client session, such as a secure connection or VPN or Unsecure, in (Col 19 line 42 to Col 20 line 40).

However, Wood does not directly discloses the “secure web pages”.

Nevertheless, Wood does disclose of accessing secure resources using the browser and implementing secure connection to the resource using encryption communication protocol, such as VPN, and SSL in (Col 7 lines 11-34, Col 7 line 58 to Col 8 line 22, and Col 18 lines 35-63).

Therefore, it would have been obvious at the time of the invention was made to one ordinary skill in the art to realize that the secure web pages are the secure resources accessing from the web browser through an encryption connection.

8. As per claims 2, and 21:

Wood discloses “The method of claim 1, wherein said method also comprises the steps of requesting said session cookie from said web client whenever said web client

Art Unit: 2135

requests access to said non-secure; web pages and verifying said requested session cookie; and requesting said authcode cookie from said web client whenever said web client requests access to said secure web pages and verifying said requested authcode cookie" in (Col 10 line 58 to Col 11 line 13 and Col 13 lines 1-19, Col 8 lines 22-49, and Col 19 line 42 to Col 20 line 40).

9. As per claims 3, 14, and 22:

Wood does not directly teach "wherein said method comprises repeatedly alternating between said secure communication protocol and said non-secure communication protocol when said web client alternates requests for access to said secure web pages and said non-secure web pages, respectively, and also repeatedly alternating between said utilizations of said authcode and said utilizations of said session code".

Nevertheless, Wood discloses a method of implementing multiple cookies with different credential and security requirement or trust level to access a certain resource of information over the web in (Col 5 lines 30-48, Col 7 line 58 to Col 8 line 23, Col 8 lines 41-55, and Col 8 line 55 to Col 9 line 25). Wood further teaches the different scenarios where each accessing request session requires a different token due to vary requirement of different trust level or credential and environmental information (i.e. encryption or non-encryption connection) (Col 7 lines 40-65, and Col 15 lines 1-57).

Therefore, it would have been obvious at the time of the invention was made to one ordinary skill in the art to realize that Wood's invention does have the capability of

alternating the usage of session code and authcode to access said non-secure communication protocol and said secure communication protocol.

10. As per claims 4, 15, and 23:

Wood does not specifically teach "wherein said alternating between said secure communication protocol and said non-secure communication protocol is facilitated by a table which keeps track of said non-secure web pages and said secure web pages".

Nevertheless, Wood does teach "The Applicant authorization service 313 interacts with application resource registry 314 to identify trust level requirements for the requested resource (and in some configurations, for a particular function or facility of the requested resource) and determines the sufficiency of a current trust level evidenced by the session credential" in (Col 17 lines 35-54). Further Wood teaches to utilize a "static or dynamic table associating trust level to authentication schemes" in Col 21 lines 24-25.

Therefore, it would have been obvious at the time of the invention was made to one ordinary skill in the art to realize that the registry 314 is stored in a table format in order to access the data easily in an organized manner.

11. As per claims 5 and 24:

Wood does not specifically disclose "wherein said web site uses said table to direct said web client to use said secure communication protocol or said non secure communication protocol depending on whether said web client requests access to said non-secure web pages or said secure web pages".

Nevertheless, Wood teaches "The authorization service 313 interacts with application resource registry 314 to identify trust level requirements for the requested resource (and in some configurations, for a particular function or facility of the requested resource) and determines the sufficiency of a current trust level evidenced by the session credential" in (Col 17 lines 35-54). Further Wood teaches of utilizing "static or dynamic table associating trust level to authentication schemes" in Col 21 lines 24-25. The credential and the trust level to access the resource requires a certain environment information, such as encrypt or non-encrypt connection communication.

Therefore, it would have been obvious at the time of the invention was made to one ordinary skill in the art to include in Wood the table to direct said web client to use a certain communication protocol.

12. As per claims 6, 16, and 25:

Wood discloses "The method of claim 6, wherein said method also comprises allowing said web client to be a guest client or a registered client" in (Col 9 lines 20-25).

13. As per claims 7, 17, and 26:

Wood discloses "The method of claim 6, wherein said method also comprises creating stored information including data contained in said session cookie, data contained in said authcode cookie and data about said web client" in (Col 19 lines 42-57).

14. As per claims 8, 18, and 27:

Wood discloses "The method of claim 7, wherein said session cookie includes a pointer and an encrypted portion, said pointer pointing to said stored information, said encrypted portion having a random portion (session ID) and a date portion" in (Col 19 lines 40-55, and Col 20 lines 40-58).

15. As per claims 9, 19, and 28:

Wood discloses "The method of claim 7, wherein said authcode cookie includes an encrypted portion, said encrypted portion having a random portion (session ID) and a date portion" in (Col 19 lines 40-55, and Col 20 lines 40-58).

16. As per claims 10, 11, 13, 29, and 30:

Wood discloses "The method of claim 8, wherein verifying said requested session cookie from said web client includes using said stored information to generate a second session cookie and comparing said second session cookie to said session cookie requested from said web client" in (Col 8 lines 41-55).

17. As per claim 12:

Wood discloses "A system, for secure session management and authentication between a web site and a web client, said system comprising a web server, a web client and a communication channel, said web server coupled to said web client via said communication channel, said web server having a web site, said web site including:

a) secure (Col 7 lines 35-67) and non-secure web pages" in (Fig. 1, Col 5 lines 1-40, Col 8 lines 23-67);

The session cookie in Wood is the session cookie that has a low credential or trust level (Col 9 lines 20-25), and the authcode cookie is also the session cookie that has a high credential or trust level and the authentication information is encrypted (Col 8 line 65 to Col 9 line 25). Wood discloses in Col 8 lines 3-18 that the environmental information of the session (i.e. browser type, encryption capability, connection type and more) is used in some configurations for mapping particular authentication mechanisms to trust levels and for authorization decisions.

“b) a non-secure communication protocol and a session cookie that is used for allowing said web client access to each one of said non-secure web pages” in (Col 8 lines 44-55); and Wood further discloses of implementing multiple cookies or tokens to allow access different credential level or trust level resources (Col 8 lines 15-55) using the environmental information of the client session in (Col 19 line 42 to Col 20 line 40). “e) a secure communication protocol and an authcode cookie that is used for allowing said web client access only to said secure web pages” in (Col 7 line 35 to Col 8 line 10).

However, Wood does not directly discloses the “secure web pages”.

Nevertheless, Wood does disclose of accessing secure resources using the browser and of implementing secure connection to the resource using encryption communication protocol, such as VPN, and SSL in (Col 7 lines 11-34, Col 7 line 58 to Col 8 line 22, and Col 18 lines 35-63).

Therefore, it would have been obvious at the time of the invention was made to one ordinary skill in the art to realize that the secure web pages are the secure resources accessing from the web browser through an encryption connection.

18. As per claim 20:

Wood discloses "A computer program embodied on a computer readable medium, said computer program providing for secure session management and authentication between a web site and a web client, said web site having secure and non-secure web pages" in (Fig. 1, Col 5 lines 1-40, Col 8 lines 23-67), said computer program adapted to:

a) use a non-secure communication protocol and a session cookie when said web client requests access to said non-secure web pages" in (Col 8 lines 44-55); Wood further discloses of implementing multiple cookies or tokens to allow access different credential level or trust level resources (Col 8 lines 15-55) using the environmental information of the client session in (Col 19 line 42 to Col 20 line 40).

"b) use a secure communication protocol and an authcode cookie whenever said web client requests access to said secure web pages;" in (Col 7 line 35 to Col 8 line 10).

The session cookie in Wood is the session cookie that has a low credential or trust level (Col 9 lines 20-25), and the authcode cookie is also the session cookie that has a high credential or trust level and the authentication information is encrypted (Col 8 line 65 to Col 9 line 25). Wood discloses in Col 8 lines 3-18 that the environmental information of the session (i.e. browser type, encryption capability, connection type and more) is used in some configurations for mapping particular authentication mechanisms to trust levels and for authorization decisions.

However, Wood does not directly discloses the "secure web pages".

Nevertheless, Wood does disclose of accessing secure resources using the browser and of implementing secure connection to the resource using encryption communication protocol, such as VPN, and SSL in (Col 7 lines 11-34, Col 7 line 58 to Col 8 line 22, and Col 18 lines 35-63).

Therefore, it would have been obvious at the time of the invention was made to one ordinary skill in the art to realize that the secure web pages are the secure resources accessing from the web browser through an encryption connection.

19. Claims 31 and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wood et al, US/6892307B1, hereinafter "Wood", in view of Reiche, US/6092196 (Cited in 892 dated 07/14/04).

20. As per claim 31:

Wood discloses "The computer program of Claim 20, wherein said computer program is adapted for creating a NAME attribute in a session cookie

a) generating a user-id; b) generating a session string (Session ID); c) generating a session timestamp;

d) appending said session timestamp to said session string to create an intermediate value" in (Col 19 lines 40-58);

However, Wood does not disclose "e) applying a one way hash function to said intermediate value to create a final value; and f) storing said final value in said NAME: attribute".

Nevertheless, Reiche teaches "e) applying a one way hash function to said intermediate value to create a final value; and f) storing said final value in said NAME attribute" in (Col 8 line 65 to Col 9 line 12).

Therefore, it is obvious at the time of the invention was made to one ordinary skill in the art to incorporate Wood's teaching of creating a NAME attribute in an session cookie and applying a one-way hash function to the intermediate value to create a final value to hide the actual information of the session to prevent hacking.

21. As per claim 33:

Wood discloses "The computer program of Claim 20, wherein said computer program is adapted to create a NAME attribute in an authcode cookie by:

- a) generating an authcode;
- "b) generating an authcode timestamp;
- c) appending said authcode timestamp to said authcode to create an intermediate value" in (Col 19 lines 42-58, and Col 20 lines 40-48);

However, Wood does not disclose "d) applying a one way hash function to said intermediate value to create a final value; and e) storing said final value in said NAME attribute".

Nevertheless, Reiche teaches "d) applying a one way hash function to said intermediate value to create a final value; and e) storing said final value in said NAME attribute" (Col 8 line 65 to Col 9 line 12).

Therefore, it is obvious at the time of the invention was made to one ordinary skill in the art to incorporate Wood's teaching of creating a NAME attribute in an authcode

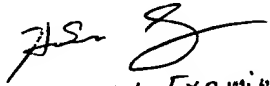
cookie and applying a one-way hash function to the intermediate value to create a final value to hide the actual information of the session to prevent hacking.

22. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Linh LD Son whose telephone number is 571-272-3856. The examiner can normally be reached on 9-6 (M-F).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Linh LD Son
Examiner
Art Unit 2135


Primary Examiner
Art Unit 2135